UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/982,711	10/18/2001	Taizo Shirai	09812.0590-00000	8666

22852 7590 04/26/2006

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
KHOSHNOODI, NADIA	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 04/26/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/982,711	SHIRAI ET AL.	
	Examiner	Art Unit	
	Nadia Khoshnoodi	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 January 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s)_____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *1/24/2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendments

Applicant's amendments/arguments filed 1/24/2006 with respect to amended claims 1, 8, 15, & 17-32 and previously presented claims 2-7, 9-14, & 16 have been fully considered but are moot in view of the new ground(s) of rejection.

Amendments to the drawings and specification filed 1/24/2006 are accepted.

Response to Arguments

Applicants contend that Hazard fails to teach or suggest a "cryptosystem unity that selectively uses a different encryption key for each sector." Furthermore, Applicants contend that Hazard discloses a method wherein the "same protection key CPi may be used to encrypt different sensitive information..." Examiner respectfully disagrees. Hazard specifically states that there are plural keys for encryption, i.e. a different encryption key, each associated with one of the items out of *n* items of sensitive information, i.e. for each sector (col. 4, lines 28-46 and col. 5, lines 1-22). Therefore, Hazard teaches a "cryptosystem unity that selectively uses a different encryption key for each sector."

Claim Rejections - 35 USC § 103

I. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

II. Claims 1-2, 5, 8, 15-18, 21, 24-25, 28, and 31-32 are rejected under 35 U.S.C. 103(a) as

being unpatentable over Hazard, United States Patent No. 6,658,566 and further in view of Sudia et al., United States Pub. No. 2005/0114666.

As per claims 1 and 17:

Hazard substantially teaches an information recording device and method for executing processing which stores data to a memory having a data storage area consisting of a plurality of blocks, each of the blocks consists of M sectors from a first sector to a M-th sector with each sector having a predetermined data capacity, where M represents a natural number (col. 5, lines 15-39 and fig. 3), said information recording device comprising a cryptosystem unit which selectively uses different encryption keys for each sectors from the first sector to the M-th sector to execute encryption processing and the cryptosystem unit executes encryption processing on data to be stored in each of the sectors (col. 5, lines 1-14 and fig. 2).

Not explicitly disclosed is a revocation list having revocation information and a block permission table for accessing a permission table that describes memory access control information. However, Sudia et al. teach a table that contains information regarding all of the possible privileges a user may have (par. 237). Furthermore, Sudia et al. teach maintaining a revocation list in order to indicate that a privilege is no longer valid (par. 244-246). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hazard et al. to have revocation information and a block permission table for accessing a permission table that describes memory access control information. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Sudia et al. suggest that incorporating a permissions table and revocation information add to the security of the system in

order to determine who may or may not gain access to specific resources at the time the user is attempting to do so in par. 237 and par. 245.

Also not explicitly disclosed is checking the integrity of the revocation list and checking the integrity of the block permission table. However, Sudia et al. teach that it is important to check the integrity of the information in the tables that ultimately allow users' access to resources in order to ensure that the permissions/revocation list is being enforced in such a way that a user exceeds their permissions/resources that they should be able to access. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hazard et al. to have an integrity unit in order to ensure the integrity of the revocation list and block permission table. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Sudia et al. suggest that the permissions and revocation information may be included in the hashed value in order to ensure the validity of the data and that the data has not been improperly modified in par. 219, par. 237, and par. 244-245.

As per claims 2 and 18:

Hazard and Sudia et al. substantially teach an information recording device and method of claim 1. Furthermore, Hazard teaches the information recording device and method wherein in said cryptosystem unit, from among M different encryption keys corresponding to M sectors, which are stored in header information corresponding to the data to be stored in said memory, one encryption key is selected in accordance with a sector in which the data is stored, and the selected encryption key is used to perform the encryption of data to be stored in each of the sectors (col. 5, lines 35-39 and fig. 3). Although the term "header information" is not

specifically used, the information is stored in such a way that it is identical to that of header information.

As per claims 5 and 21:

Hazard and Sudia et al. substantially teach an information recording device and method of claim 1. Furthermore, Hazard teaches the information recording device and method wherein, in said cryptosystem unit, the encryption processing for the first sector to the M-th sector is executed as single-DES encryption processing using different encryption keys for the sectors (col. 4, lines 32-46).

As per claims 8 and 24:

Hazard substantially teaches the information recording device and method for executing processing which reads data from a memory having a data storage area consisting of a plurality of blocks, each of which consists of the first sector to the M-th sector which each have a predetermined data capacity, where M represents a natural number (col. 5, lines 15-39 and fig. 3), said information playback device comprising a cryptosystem unit which selectively uses different decryption keys for the first sector to M-th sector to execute decryption processing and which executes decryption processing on data stored in each of the sectors (col. 4, lines 32-46, col. 5, lines 1-14, and fig. 2). Not explicitly disclosed is a revocation list having revocation information and a block permission table for accessing a permission table that describes memory access control information. However, Sudia et al. teach a table that contains information regarding all of the possible privileges a user may have (par. 237). Furthermore, Sudia et al. teach maintaining a revocation list in order to indicate that a privilege is no longer valid (par. 244-246). Therefore, it would have been obvious to a person in the art at the time the invention

was made to modify the method disclosed in Hazard et al. to have revocation information and a block permission table for accessing a permission table that describes memory access control information. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Sudia et al. suggest that incorporating a permissions table and revocation information add to the security of the system in order to determine who may or may not gain access to specific resources at the time the user is attempting to do so in par. 237 and par. 245.

Also not explicitly disclosed is checking the integrity of the revocation list and checking the integrity of the block permission table. However, Sudia et al. teach that it is important to check the integrity of the information in the tables that ultimately allow users' access to resources in order to ensure that the permissions/revocation list is being enforced in such a way that a user exceeds their permissions/resources that they should be able to access. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hazard et al. to have an integrity unit in order to ensure the integrity of the revocation list and block permission table. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Sudia et al. suggest that the permissions and revocation information may be included in the hashed value in order to ensure the validity of the data and that the data has not been improperly modified in par. 219, par. 237, and par. 244-245.

As per claims 9 and 25:

Hazard and Sudia et al. substantially teach an information recording device and method of claim 8. Furthermore, Hazard teaches the information recording device and method wherein,

in said cryptosystem unit, from among M different decryption keys corresponding to M sectors, which are stored in header information corresponding to data stored in said memory, one decryption key is selected in accordance with a sector in which the data is stored, and the selected decryption key is used to perform the decryption of data stored in each of the sectors (col. 4, lines 32-46, col. 5, lines 35-39 and fig. 3). Although the term "header information" is not specifically used, the information is stored in such a way that it is identical to that of header information.

As per claims 12 and 28:

Hazard and Sudia et al. substantially teach an information recording device and method of claim 8. Furthermore, Hazard teaches an information playback device and method wherein, in said cryptosystem unit, the decryption processing for the first sector to the M-th sector is executed as single-DES decryption processing using different decryption keys for the sectors (col. 4, lines 32-46).

As per claim 15:

Hazard substantially teaches an information recording medium having a data storage area consisting of a plurality of blocks, each of which consists of the first sector to the M-th sector which each have a predetermined data capacity, where M represents a natural number (col. 5, lines 15-39 and fig. 3), wherein a plurality of different cryptographic keys which are selectable for the sectors are stored as header information of data stored in said data storage area (col. 5, lines 35-39). Although the term "header information" is not specifically used, the information is stored in such a way that it is identical to that of header information. Not explicitly disclosed is a revocation list having revocation information and a block permission table for accessing a

permission table that describes memory access control information. However, Sudia et al. teach a table that contains information regarding all of the possible privileges a user may have (par. 237). Furthermore, Sudia et al. teach maintaining a revocation list in order to indicate that a privilege is no longer valid (par. 244-246). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hazard et al. to have revocation information and a block permission table for accessing a permission table that describes memory access control information. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Sudia et al. suggest that incorporating a permissions table and revocation information add to the security of the system in order to determine who may or may not gain access to specific resources at the time the user is attempting to do so in par. 237 and par. 245.

Also not explicitly disclosed is checking the integrity of the revocation list and checking the integrity of the block permission table. However, Sudia et al. teach that it is important to check the integrity of the information in the tables that ultimately allow users' access to resources in order to ensure that the permissions/revocation list is being enforced in such a way that a user exceeds their permissions/resources that they should be able to access. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hazard et al. to have an integrity unit in order to ensure the integrity of the revocation list and block permission table. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Sudia et al. suggest that the permissions and revocation information

may be included in the hashed value in order to ensure the validity of the data and that the data has not been improperly modified in par. 219, par. 237, and par. 244-245.

As per claim 16:

Hazard and Sudia et al. substantially teach an information recording device and method of claim 15. Furthermore, Hazard teaches an information recording medium, wherein said plurality of different cryptographic keys are M different encryption keys corresponding to the M sectors (col. 5, lines 1-14 and fig. 2).

As per claim 31:

Hazard substantially teaches a program providing medium for providing a computer program which controls a computer system to execute processing which stores data in a memory having a data storage area consisting of a plurality of blocks, each of which consists of the first sector to the M-th sector which each have a predetermined data capacity, where M represents a natural number (col. 5, lines 15-39 and fig. 3), said computer program comprising a data-encrypting step in which encryption processing on data to be stored in the sectors is executed by performing encryption using encryption keys selected for the first sector to the M-th sector (col. 5, lines 1-14 and fig. 2).

Not explicitly disclosed is a revocation list having revocation information and a block permission table for accessing a permission table that describes memory access control information. However, Sudia et al. teach a table that contains information regarding all of the possible privileges a user may have (par. 237). Furthermore, Sudia et al. teach maintaining a revocation list in order to indicate that a privilege is no longer valid (par. 244-246). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the

method disclosed in Hazard et al. to have revocation information and a block permission table for accessing a permission table that describes memory access control information. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Sudia et al. suggest that incorporating a permissions table and revocation information add to the security of the system in order to determine who may or may not gain access to specific resources at the time the user is attempting to do so in par. 237 and par. 245.

Also not explicitly disclosed is checking the integrity of the revocation list and checking the integrity of the block permission table. However, Sudia et al. teach that it is important to check the integrity of the information in the tables that ultimately allow users' access to resources in order to ensure that the permissions/revocation list is being enforced in such a way that a user exceeds their permissions/resources that they should be able to access. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hazard et al. to have an integrity unit in order to ensure the integrity of the revocation list and block permission table. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Sudia et al. suggest that the permissions and revocation information may be included in the hashed value in order to ensure the validity of the data and that the data has not been improperly modified in par. 219, par. 237, and par. 244-245.

As per claim 32:

Hazard substantially teaches program providing medium for providing a computer program which controls a computer system to execute processing which reads data from a

memory having a data storage area consisting of a plurality of blocks, each of which consists of the first sector to the M-th sector which each have a predetermined data capacity, where M represents a natural number (col. 5, lines 15-39 and fig. 3), said computer program comprising a data-decrypting step in which decryption of data stored in each of the sectors is performed by executing decryption processing using decryption keys selected in accordance with the first sector to the M-th sector (col. 4, lines 32-46, col. 5, lines 1-14, and fig. 2).

Not explicitly disclosed is a revocation list having revocation information and a block permission table for accessing a permission table that describes memory access control information. However, Sudia et al. teach a table that contains information regarding all of the possible privileges a user may have (par. 237). Furthermore, Sudia et al. teach maintaining a revocation list in order to indicate that a privilege is no longer valid (par. 244-246). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hazard et al. to have revocation information and a block permission table for accessing a permission table that describes memory access control information. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Sudia et al. suggest that incorporating a permissions table and revocation information add to the security of the system in order to determine who may or may not gain access to specific resources at the time the user is attempting to do so in par. 237 and par. 245.

Also not explicitly disclosed is checking the integrity of the revocation list and checking the integrity of the block permission table. However, Sudia et al. teach that it is important to check the integrity of the information in the tables that ultimately allow users' access to

resources in order to ensure that the permissions/revocation list is being enforced in such a way that a user exceeds their permissions/resources that they should be able to access. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hazard et al. to have an integrity unit in order to ensure the integrity of the revocation list and block permission table. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Sudia et al. suggest that the permissions and revocation information may be included in the hashed value in order to ensure the validity of the data and that the data has not been improperly modified in par. 219, par. 237, and par. 244-245.

III. Claims 3-4, 6, 10-11, 13, 19-20, 22, 26-27, and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hazard, United States Patent No. 6,658,566 and Sudia et al., United States Pub. No. 2005/0114666 as applied to claims 1, 8, 17, and 24 above, and further in view of Dilkie et al., United States Patent No. 6,341,164.

As per claims 3 and 19:

Hazard and Sudia et al. substantially teach an information recording device and method, as applied to claims 1 and 17 above. Not explicitly disclosed is the device/method wherein, in said cryptosystem unit, from among M different encryption keys corresponding to M sectors, which are stored in header information corresponding to the data to be stored in said memory, a set of at least two encryption keys is selected in accordance with a sector in which the data is stored, and the selected encryption keys are used to perform the encryption of data to be stored in each of the sectors. However, Hazard teaches the use of single-DES encryption (col. 4, lines 32-46). Furthermore, Dilkie et al. teach the use of triple-DES which uses at least 2 keys for

encryption. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the device/method disclosed in Hazard to use triple-DES for the encryption processing, thereby using at least 2 keys for encryption. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Dilkie et al. in col. 2, lines 48-54.

As per claims 4 and 20:

Hazard and Sudia et al. substantially teach an information recording device and method, as applied to claims 1 and 17 above. Not explicitly disclosed is the device/method wherein, in said cryptosystem unit, from among P different encryption keys in which the number P differs from the number M, at least one encryption key is selected in accordance with a sector in which the data is stored, and the selected at least one encryption key is used to perform the encryption of data to be stored in each of the sectors.

However, Dilkie et al. teach that from among P different encryption keys, where P differs from the number M, at least one encryption key is selected from a key package to use for encryption purposes. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the device/method disclosed in Hazard to choose at least one encryption key for encrypting data to be stored in each of the sectors from P different keys, where the number P differs from the number M. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Dilkie et al. in col. 4, lines 1-37 and col. 4, line 51- col. 2, line 6.

As per claims 6 and 22:

Hazard and Sudia et al. substantially teach an information recording device and method, as applied to claims 1 and 17 above. Not explicitly disclosed is the information recording device wherein, in said cryptosystem unit, the encryption processing for the first sector to the M-th sector is executed as triple-DES encryption processing using at lest two different encryption keys for each of the sectors. However, Dilkie et al. teaches the use of a triple-DES encryption processing. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the device/method disclosed in Hazard to use triple-DES for the encryption processing. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Dilkie et al. in col. 2, lines 48-54.

As per claims 10 and 26:

Hazard and Sudia et al. substantially teach an information playback device and method, as applied to claims 8 and 24 above. Not explicitly disclosed is the device/method wherein an information playback device and method wherein, in said cryptosystem unit, from among M different decryption keys corresponding to M sectors, which are stored in header information corresponding to data stored in said memory, a set of at least two decryption keys is selected in accordance with a sector in which data is stored, and the selected encryption keys are used to perform the decryption of data stored in each of the sectors. However, Hazard teaches the use of single-DES decryption (col. 4, lines 32-46 and col. 4, lines 32-46). Furthermore, Dilkie et al. teach the use of triple-DES which uses at least 2 keys for decryption. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the device/method disclosed in Hazard to use triple-DES for the decryption processing, thereby

using at least 2 keys for decryption. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Dilkie et al. in col. 2, lines 48-54.

As per claims 11 and 27:

Hazard and Sudia et al. substantially teach an information playback device and method, as applied to claims 1 and 17 above. Not explicitly disclosed is the device/method wherein, in said cryptosystem unit, from among P different decryption keys in which the number P differs from the number M, at least one decryption key is selected in accordance with a sector in which data is stored, and the selected at least one decryption key is used to perform the decryption of data stored in each of the sectors.

However, Dilkie et al. teach that from among P different encryption keys, where P differs from the number M, at least one encryption key is selected from a key package to use for encryption purposes. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the device/method disclosed in Hazard to choose at least one decryption key based on the encryption keys stored in each of the sectors from P different keys, where the number P differs from the number M. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Dilkie et al. in col. 4, lines 1-37, col. 4, line 51-col. 2, line 6, and col. 5, lines 61-67).

As per claims 13 and 29:

Hazard and Sudia et al. substantially teach an information playback device and method, as applied to claims 8 and 24 above. Not explicitly disclosed is the information playback device

wherein, in said cryptosystem unit, the decryption processing for the first sector to the M-th sector is executed as triple-DES decryption processing using at lest two different decryption keys for each of the sectors. However, Dilkie et al. teaches the use of a triple-DES decryption processing. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the device/method disclosed in Hazard to use triple-DES for the decryption processing. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Dilkie et al. in col. 2, lines 48-54.

IV. Claims 7, 14, 23, and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hazard, United States Patent No. 6,658,566 and Sudia et al., United States Pub. No. 2005/0114666 as applied to claims 1, 8, 17, and 24 above, and further in view of Schneier, *Applied Cryptography*.

As per claims 7 and 23:

Hazard and Sudia et al. substantially teach an information recording device and method, as applied to claims 1 and 17 above. Furthermore, Hazard teaches the use of header information used to store the key as encrypted by an encryption algorithm, as well as other relevant information (col. 8, lines 15-39). Not explicitly disclosed is the device/method wherein said cryptosystem unit selectively executes one of sector-independent encryption processing in which in accordance with an encryption format type stored in header information corresponding to the data to be stored in said memory, the entirety of the data is encrypted in a single encryption mode, and sector-dependent encryption processing in which in accordance with the encryption format type, the data is encrypted by using encryption keys which are selected for the sectors.

However, Schneier teaches using sector-independent encryption processing where the entirety of data is encrypted in a single encryption mode, and sector-dependent encryption processing where the data is encrypted by using encryption keys that are selected for the sectors. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the device/method disclosed in Hazard to store the encryption format type in the header information to designate a sector-dependent or sector-independent encryption format. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Schneier on pages 221, lines 8-12 and 222, lines 24-43.

As per claims 14 and 30:

Hazard and Sudia et al. substantially teach an information playback device and method, as applied to claims 8 and 24 above. Furthermore, Hazard teaches the use of header information used to store the key as encrypted by an encryption algorithm, as well as other relevant information (col. 8, lines 15-39). Not explicitly disclosed is the device/method wherein said cryptosystem unit selectively executes one of sector-independent decryption processing in which in accordance with an encryption format type stored in header information corresponding to data stored in said memory, the entirety of the data is decrypted in a single decryption mode, and sector-dependent decryption processing in which in accordance with the encryption format type, the data is decrypted by using decryption keys which are selected for the sectors.

However, Schneier teaches using sector-independent decryption processing where the entirety of data is decrypted in a single decryption mode, and sector-dependent decryption processing where the data is decrypted by using decryption keys that are selected for the sectors.

Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the device/method disclosed in Hazard to store the encryption format type in the header information to designate a sector-dependent or sector-independent decryption format. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Schneier on pages 221, lines 8-12 and 222, lines 24-43.

**References Cited, Not Used*

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

1. US Patent No. 5,892,900
2. US Pub. No. 2006/0021064
3. US Pub. No. 2006/0053077

The above references have been cited because they are relevant due to the manner in which the invention has been claimed.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Nadia Khoshnoodi
Examiner
Art Unit 2137
4/20/2006

NK

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER